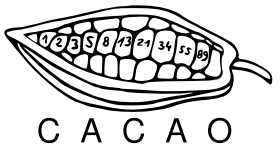
Applications algorithmiques des courbes elliptiques

Emmanuel Thomé,
Projet CACAO, INRIA Lorraine

INRIA LORRAINE



Plan

1. **Factorisation par la méthode des courbes elliptiques**
2. **Applications immédiates des courbes en cryptologie**
3. **Couplages**

1. **Factorisation par la méthode des courbes elliptiques**
   - $p-1$
   - $p+1$
   - **ECM – Phase 1**
   - **Phase 2**
2. **Applications immédiates des courbes en cryptologie**
3. **Couplages**

Contexte

Factoriser des entiers est un problème difficile.

Deux types d'algorithmes pour trouver un facteur p d'un nombre N.

- Algorithmes qui dépendent de la taille de N :
  Crible quadratique (QS), Crible algébrique (NFS).

$$\text{NFS :} \quad \exp\left(\tilde{O}\left(\sqrt[3]{\log N}\right)\right).$$

- Algorithmes qui dépendent de la taille de p :
  Pollard ρ, $p-1$, $p+1$, ECM (Elliptic curve method).

$$\text{ECM :} \quad \exp\left(\tilde{O}\left(\sqrt{\log p}\right)\right).$$

  $\Rightarrow$ particulièrement bien adapté pour des facteurs petits ou moyens.

Le commencement

Avant ECM, on ne fait pas l'économie de regarder l'algorithme $p-1$.

Principe :

- On a N.
- « À tout hasard », existe-t-il p tel que :
  $p \mid N$ et tous les facteurs premiers de $p-1$ sont petits ?

Méthode $p-1$

Si $N = pq$, on a un isomorphisme : (on ne sait pas le calculer !)

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^* & \longleftrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \\ x & \longleftrightarrow & (x \bmod p, x \bmod q). \end{array}$$

Supposons $p-1 \mid \Gamma$, avec $\Gamma = B_1$! (ou bien $\Gamma = \prod_{\pi < B_1} \pi^{\left\lfloor \frac{\log B_1}{\log \pi} \right\rfloor}$).

Alors pour $x \in (\mathbb{Z}/N\mathbb{Z})^*$, puisque l'ordre de $(\mathbb{Z}/p\mathbb{Z})^*$ est $p-1$:

$$x^\Gamma \bmod N \longleftrightarrow (1, *).$$

Méthode $p-1$

Si $N=pq$, on a un isomorphisme : (on ne sait pas le calculer !)

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^* & \longleftrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \\ x & \longleftrightarrow & (x \bmod p, x \bmod q). \end{array}$$

Supposons $p-1 \mid \Gamma$, avec $\Gamma = B_1$! (ou bien $\Gamma = \prod_{\pi<B_1} \pi^{\left\lfloor \frac{\log B_1}{\log \pi} \right\rfloor}$).

Alors pour $x \in (\mathbb{Z}/N\mathbb{Z})^*$, puisque l'ordre de $(\mathbb{Z}/p\mathbb{Z})^*$ est $p-1$:

$$x^\Gamma \bmod N \longleftrightarrow (1, *).$$

$\Rightarrow$ **ALGO** :
- x entier aléatoire $\bmod N$.
- Calculer $y = x^\Gamma \bmod N$.
- Tester si $\gcd(y-1, N) \neq 1$.

Méthode $p-1$ (suite)

Gros problème de la méthode $p-1$: c'est un fusil à un coup.

Si $p-1$ n'a pas assez de petits facteurs, on a perdu.

A-t-on droit à une deuxième chance ?

Méthode $p-1$ (suite)

Gros problème de la méthode $p-1$: c'est un fusil à un coup.

Si $p-1$ n'a pas assez de petits facteurs, on a perdu.

A-t-on droit à une deuxième chance ?

Essayons $p+1 \Rightarrow$ « À tout hasard », existe-t-il p tel que :
$p \mid N$ et tous les facteurs premiers de $p+1$ sont petits ?

Méthode $p+1$

- On travaille dans $T_N = \left\{ (x,y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x^2 - Dy^2 = 1 \right\},\ D \in \mathbb{Z}$.
- On a un morphisme (pas plus calculable que l'autre) :

$$\begin{array}{ccc} T_N & \longrightarrow\!\!\!\!\!\rightarrow & T_p \cong \begin{cases} \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \\ \mathbb{F}_p^* \end{cases} \\ (x,y) & \longmapsto & (x \bmod p, y \bmod p). \end{array}$$

Méthode $p+1$

- On travaille dans $T_N = \left\{(x,y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x^2 - Dy^2 = 1\right\}$, $D \in \mathbb{Z}$.
- On a un morphisme (pas plus calculable que l'autre) :

$$T_N \twoheadrightarrow T_p \cong \begin{cases} \mathbb{F}_{p^2}^*/\mathbb{F}_p^* & \text{(cas intéressant)} \\ \cancel{\mathbb{F}_p^*} \end{cases}$$

$$(x,y) \longmapsto (x \bmod p, y \bmod p).$$

On s'intéresse aux cas où $D \neq \square \bmod p$ (1 cas sur 2).

- Point de départ $(x_1, y_1) \in T_N$; on note $\alpha = x_1 + y_1\sqrt{D}$.
- On étudie (x_n, y_n) tels que $x_n + y_n\sqrt{D} = \alpha^n$.
- Modulo p, comme $D \neq \square$, on a $\alpha^p = \bar{\alpha} = x_1 - y_1\sqrt{D}$. Donc $\boxed{\alpha^{p+1} = 1}$.

Méthode $p+1$ (suite)

Supposons $p+1 \mid \Gamma$, avec $\Gamma = B_1$! (ou bien $\Gamma = \prod_{\pi < B_1} \pi^{\left\lfloor \frac{\log B_1}{\log \pi} \right\rfloor}$).

Alors puisque $\alpha^{(p+1)} = 1 \bmod p$, on a $(x_\Gamma, y_\Gamma) = (1,0) \bmod p$,

$$\begin{array}{ccc} T_N & \twoheadrightarrow & T_p \\ (x_\Gamma, y_\Gamma) & \mapsto & (1,0). \end{array}$$

Méthode $p+1$ (suite)

Supposons $p+1 \mid \Gamma$, avec $\Gamma = B_1$! (ou bien $\Gamma = \prod_{\pi < B_1} \pi^{\left\lfloor \frac{\log B_1}{\log \pi} \right\rfloor}$).

Alors puisque $\alpha^{(p+1)} = 1 \bmod p$, on a $(x_\Gamma, y_\Gamma) = (1,0) \bmod p$,

$$\begin{array}{ccc} T_N & \longrightarrow\!\!\!\!\!\rightarrow & T_p \\ (x_\Gamma, y_\Gamma) & \longmapsto & (1,0). \end{array}$$

$\Rightarrow$ **ALGO** :

- Choix de D, x_1, y_1 $\quad (x_1 = \frac{P}{2},\ y_1 = \frac{1}{2},\ D = P^2 - 4)$.
- Calculer (x_Γ, y_Γ).
- Tester si $\gcd(x_\Gamma - 1, N) \neq 1$.
- (astuces de calcul possibles).

Méthode $p+1$ – calculer x_n

On a $\alpha = x_1 + y_1\sqrt{D}$. Soit $\beta = \bar{\alpha} = x_1 - y_1\sqrt{D}$. On a $\alpha\beta = 1$, et :

$$v_n = 2x_n = \alpha^n + \beta^n.$$

$$v_{m+n} = \alpha^{m+n} + \beta^{m+n} = v_m v_n - v_{m-n}.$$

Pour calculer v_n, on calcule $\{v_n, v_{n+1}\}$.

$$\{v_n, v_{n+1}\} \to \{v_{2n}, v_{2n+1}\}.$$

$$v_{2n} = v_n^2 - v_0,$$

$$v_{2n+1} = v_n v_{n+1} - v_1.$$

$$\{v_n, v_{n+1}\} \to \{v_{2n+1}, v_{2n+2}\}.$$

$$v_{2n+1} = v_n v_{n+1} - v_1,$$

$$v_{2n+2} = v_{n+1}^2 - v_0.$$

Méthode similaire à l'exponentiation binaire

$p+1, p-1, \ldots$

Comment aller plus loin (pour augmenter les chances de succès) ?

- méthode $\Phi_k(p)$; rigolo, mais compliqué et peu efficace.
- ECM (Elliptic curve method).

Principe d'ECM :

- Construire une structure $X(N)$ qui se projette en $X(p)$,
  et tel que si $x \mapsto$ élt. neutre $\in X(p)$, alors on peut identifier p.
- Espérer que $X(p)$ est d'ordre friable.
- Là où $p-1$ et $p+1$ n'offrent qu'une seule structure X,
  ECM en offre une ribambelle : des courbes elliptiques.

ECM en un transparent

On connaît N, ou cherche $p \mid N$. On fait « comme si » $\mathbb{Z}/N\mathbb{Z}$ était un corps (en cas de problème, on a un facteur).

- Choisir une courbe elliptique E au hasard, et un point P dessus.
- On calcule $Q = \Gamma P$, avec $\Gamma = \prod_{\pi < B_1} \pi^{\left\lfloor \frac{\log B_1}{\log \pi} \right\rfloor}$.
- Si $\#E(\mathbb{F}_p) \mid \Gamma$, ça va se voir ; sinon on change de courbe.

ECM en un transparent

On connaît N, ou cherche $p \mid N$. On fait « comme si » $\mathbb{Z}/N\mathbb{Z}$ était un corps (en cas de problème, on a un facteur).

- Choisir une courbe elliptique E au hasard, et un point P dessus.
- On calcule $Q = \Gamma P$, avec $\Gamma = \prod_{\pi < B_1} \pi^{\left\lfloor \frac{\log B_1}{\log \pi} \right\rfloor}$.
- Si $\#E(\mathbb{F}_p) \mid \Gamma$, ça va se voir ; sinon on change de courbe.

En fait ça tient même en un demi transparent

Un peu de détails

- Une courbe au hasard $\Rightarrow$ Pourquoi pas $y^2 = x^3 + ax + b$ pour a, b aléatoires ?

Un peu de détails

- Une courbe au hasard $\Rightarrow$ Pourquoi pas $y^2 = x^3 + ax + b$ pour a, b aléatoires ?
- Attention : N pas premier ; difficile de trouver P sur la courbe.
- Beaucoup plus simple de choisir E et P en même temps.

Calcul de $Q = \Gamma P$

On travaille modulo N, avec à l'esprit :

$$\begin{array}{ccc} E(\mathbb{Z}/N\mathbb{Z}) & \twoheadrightarrow & E(\mathbb{F}_p) \\ (x, y) & \longmapsto & (x \bmod p, y \bmod p). \end{array}$$

Calcul de $Q = \Gamma P$

On travaille modulo N, avec à l'esprit :

$$\begin{array}{ccc} E(\mathbb{Z}/N\mathbb{Z}) & \twoheadrightarrow & E(\mathbb{F}_p) \\ \cancel{(x,y) \longmapsto (x \bmod p, y \bmod p).} & & \\ (x:y:z) & \longmapsto & (x \bmod p : y \bmod p : z \bmod p). \end{array}$$

- Les coordonnées projectives $(x : y : z)$ évitent les divisions,
- L'élément neutre $\bmod p$: $O_{E(\mathbb{F}_p)} = (0 : 1 : 0)$.
- Le « ça va se voir » : on atteint $(x : y : z)$ tel que $z \equiv 0 \bmod p$.
- Comme pour $p \pm 1$, ça se détecte par un $\gcd$.

Analyse à la louche d'ECM

C'est une question de friabilité (avoir des petits facteurs).

$$L_x[\alpha; c] \stackrel{\text{def}}{=\!=} \exp\left(c(\log x)^{\alpha}(\log\log x)^{1-\alpha}\right).$$

On a le résultat suivant :
$Y \in \tilde{O}(L_x[\alpha; u])$ est $\tilde{O}(L_x[\beta; v])$-friable avec proba. $\tilde{O}(L_x[\alpha-\beta; -(\alpha-\beta)\frac{u}{v}])$.

Analyse à la louche d'ECM

C'est une question de friabilité (avoir des petits facteurs).

$$L_x[\alpha; c] \stackrel{\text{def}}{=} \exp\left(c(\log x)^{\alpha}(\log\log x)^{1-\alpha}\right).$$

On a le résultat suivant :
$Y \in \tilde{O}(L_x[\alpha; u])$ est $\tilde{O}(L_x[\beta; v])$-friable avec proba. $\tilde{O}(L_x[\alpha-\beta; -(\alpha-\beta)\frac{u}{v}])$.

- Ici $Y = \#E(\mathbb{F}_p) \in [p+1-2\sqrt{p}, p+1+2\sqrt{p}] \Rightarrow Y \in \tilde{O}(L_p[1;1])$.
- Soit $T = L_p[1/2; 1/\sqrt{2}]$. On fixe $B_1 \in \tilde{O}(T)$.
  On passe un temps $\tilde{O}(T)$ à calculer ΓP. On gagne avec proba $\tilde{O}(1/T)$.
- Si on fait cela pour $\tilde{O}(T)$ courbes :
  on gagne avec proba $\to 1$ (si p existe), en temps :

$$O(T^2) = L_p[1/2; \sqrt{2}].$$

ECM, le retour de la suite de. . .

Ce n'est pas fini !

ECM : on « gagne » si $\#E(\mathbb{F}_p)$ est friable (que des petits facteurs).

Et si jamais $\#E(\mathbb{F}_p) =$ petit $\times$ petit $\times \cdots \times$ petit $\times$ gros ?

ECM, le retour de la suite de. . .

Ce n'est pas fini !

ECM : on « gagne » si $\#E(\mathbb{F}_p)$ est friable (que des petits facteurs).

Et si jamais $\#E(\mathbb{F}_p) =$ petit $\times$ petit $\times \cdots \times$ petit $\times$ gros ?

- On a fixé B_1 la limite de ce qui était petit.
- Fixons B_2 la limite de ce qui est moyen.
- On va voir comment traiter le cas
  $\#E(\mathbb{F}_p) =$ petit $\times$ petit $\times \cdots \times$ petit $\times$ moyen

Phase 2

- On a calculé $Q = \Gamma P$. Hélas $Q \not\mapsto O_{E(\mathbb{F}_p)}$.
- On espère qu'il existe un nombre premier q tel que :
  - $B_1 \leq q < B_2$,
  - $qQ \mapsto O_{E(\mathbb{F}_p)}$.

  On pourrait ainsi récupérer le facteur p ($\mathrm{pgcd}(z, N) \neq 1$).
- Comment faire ?

Phase 2 – naïf

- On calcule qQ pour tous les nombres premiers dans $[B_1, B_2]$.

Phase 2 – naïf

- On calcule qQ pour tous les nombres premiers dans $[B_1, B_2]$.
- Il faut le faire en calculant $q_{i-1}Q + (q_i - q_{i-1})Q$.
- Ce faisant, on « touche » un q_i en une addition sur la courbe (car l'ensemble $\{q_i - q_{i-1}\}$ est petit).
- Coût $O\left(\frac{B_2}{\log B_2}\right)$.

Phase 2 – naïf

- On calcule qQ pour tous les nombres premiers dans $[B_1, B_2]$.
- Il faut le faire en calculant $q_{i-1}Q + (q_i - q_{i-1})Q$.
- Ce faisant, on « touche » un q_i en une addition sur la courbe (car l'ensemble $\{q_i - q_{i-1}\}$ est petit).
- Coût $O\left(\frac{B_2}{\log B_2}\right)$.

On peut faire beaucoup mieux. Complexité $O\left(\sqrt{B_2}\log B_2\right)$. Ingrédients :

- « pas de bébé, pas de géant »
- évaluation multipoints, interpolation.
- FFT.

ECM en pratique

- ECM est très adapté pour trouver des facteurs moyens.
- Pour chercher les facteurs d'un nombre arbitraire, on essaie dans cet ordre :
  - Pollard ρ.
  - ECM.
  - GNFS.
- Plus grand facteur trouvé par ECM : 67 chiffres.
- Les facteurs dans les 40-50 chiffres sont courants.

1. Factorisation par la méthode des courbes elliptiques
2. Applications immédiates des courbes en cryptologie
   - Arithmétique rapide
   - Difficulté du log. discret
   - Échange de clés – chiffrement – signature
3. Couplages

La liste de courses

Crypto à base de courbes elliptiques : crypto dans des groupes.

Il faut :

- Un groupe G.
- Une représentation efficace des éléments,
  idéalement en $\log_2 \#\mathsf{G}$ bits.
- Une arithmétique efficace dans ce groupe : $(x + y, nx, x \stackrel{?}{=} y)$.
- Un algorithme pour calculer le cardinal du groupe.
- Des résultats sur la difficulté du logarithme discret dans ce groupe.

La liste de courses

Crypto à base de courbes elliptiques : crypto dans des groupes.

Il faut :

- Un groupe G.
- Une représentation efficace des éléments,

  idéalement en $\log_2 \#\mathsf{G}$ bits.

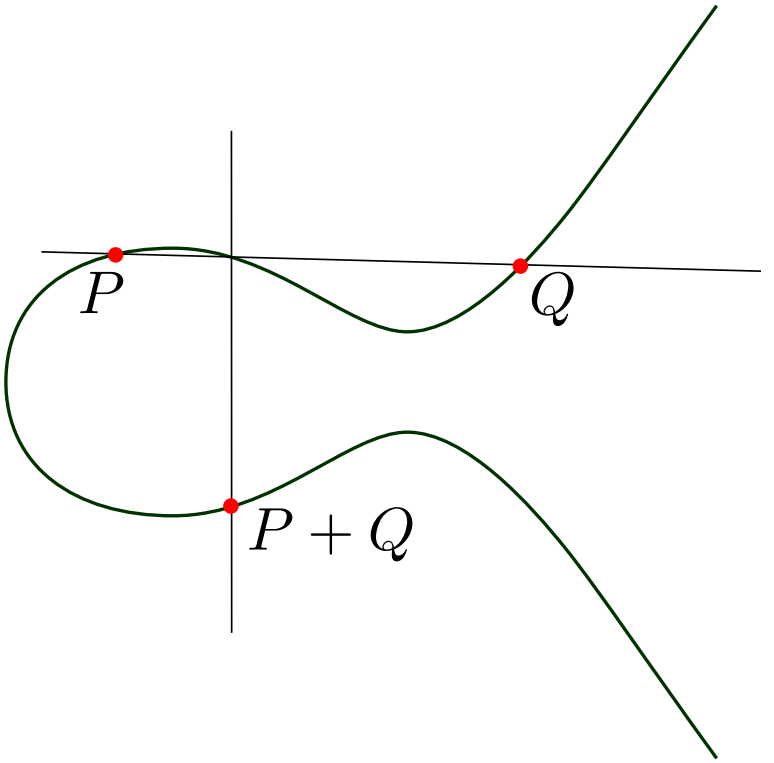
1. Une arithmétique efficace dans ce groupe : $(x + y, nx, x \stackrel{?}{=} y)$.

- Un algorithme pour calculer le cardinal du groupe.

2. Des résultats sur la difficulté du logarithme discret dans ce groupe.

Arithmétique sur les courbes elliptiques

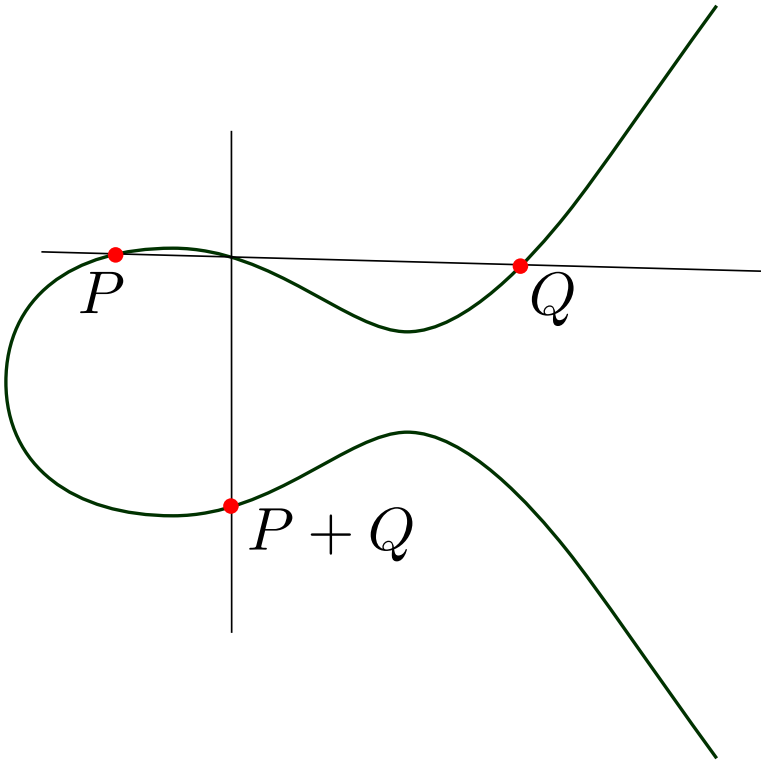
On a déjà vu comment on faisait (exposé GH).



problème avec les coordonnées affines : il y a des inversions.

Arithmétique sur les courbes elliptiques

On a déjà vu comment on faisait (exposé GH).



problème avec les coordonnées affines : il y a des inversions.

Et les inversions, c'est cher.

Éliminer les inversions

Plusieurs approches sont possibles. Ici : « Montgomery ladder ».

- On oublie les coordonnées y. On manipule des $\pm P$.
- On a une formule $\pm(m+n)P = F(\pm mP, \pm nP, \pm(m-n)P)$.

Éliminer les inversions

Plusieurs approches sont possibles. Ici : « Montgomery ladder ».

- On oublie les coordonnées y. On manipule des $\pm P$.
- On a une formule $\pm(m+n)P = F(\pm mP, \pm nP, \pm(m-n)P)$.
- Miracle : cette formule est très simple.
  Sur $y^2 = x^3 + Ax^2 + x$:

$$x_{m+n}x_{m-n} = \left(\frac{x_m x_n - 1}{x_m - x_n}\right)^2.$$

(normalement) ça rappelle quelque chose.

En coordonnées projectives (x devient $\frac{x}{z}$, points $\pm nP = (x_n :: z_n)$) :

$$x_{m+n} = (x_m x_n - z_m z_n)^2 z_{m-n},$$
$$z_{m+n} = (x_m z_n - x_n z_m)^2 x_{m+n}.$$

Montgomery ladder, calcul de $\pm nP$

On a deux formules :
- $\pm(m+n)P = F(\pm mP, \pm nP, \pm(m-n)P)$.
- $\pm 2nP = G(\pm nP)$ (qui dépend de A).

Pour calculer $\pm nP$, on calcule $\{\pm nP, \pm(n+1)P\}$.

$\{(2n)P, (2n+1)P\}$.

$$(2n)P = G(nP),$$
$$(2n+1)P = F(nP, (n+1)P, P).$$

$\{(2n+1)P, (2n+2)P\}$.

$$(2n+1)P = F(nP, (n+1)P, P),$$
$$(2n+2)P = G((n+1)P).$$

Méthode similaire à l'exponentiation binaire

Montgomery ladder, suite et fin

En utilisant cette méthode, sur la courbe

$$y^2 = x^3 + 486662x^2 + x \quad \text{sur } \mathrm{GF}(2^{255} - 19),$$

on calcule nP en $200\mu s$ (Opteron 2.4GHz).

Autres avantages :

- Pas d'inversion – peu d'opérations.
- Résiste aux *side-channel attacks*.

Moralité : on sait calculer vite

(et on calcule de la même façon pour ECM)

Le problème du log. discret

groupe $\Rightarrow$ problème du logarithme discret :
Étant donnés P et $Q = xP$, retrouver x.

version multiplicative : $(a, b = a^x) \rightarrow x)$

Quid de LD sur les courbes elliptiques ?

LD sur les courbes elliptiques

Sur n'importe quel groupe G, on sait résoudre LD en temps $O\left(\sqrt{\#\mathsf{G}}\right)$.

Sur les courbes elliptiques : pas mieux (hors cas patho).

$\Rightarrow$ considérablement plus résistant que d'autres groupes.

Comparaison : corps finis, LD en $\tilde{O}\left(L_{\#\mathsf{G}}\left[\frac{1}{3}; c\right]\right)$, avec

$$L_{\#\mathsf{G}}\left[\frac{1}{3}; c\right] = \exp\left(c(\log \#\mathsf{G})^{1/3}(\log\log \#\mathsf{G})^{2/3}\right)$$

(= entre polynomial et exponentiel).

LD sur les courbes elliptiques (suite)

Problèmes LD résolus en pratique :

- Courbes elliptiques : $\#\mathsf{G} \approx 2^{109}$ (2004).
- Corps finis.
  - $\mathbb{F}_p^*$: $\#\mathsf{G} \approx 2^{531}$ (2007).
  - $\mathbb{F}_{2^n}^*$: $\#\mathsf{G} \approx 2^{613}$ (2005).

L'écart est manifeste.

LD est très difficile sur les courbes elliptiques.

Pour être tranquille, on prend E sur $\mathbb{F}_q$ avec :

- $q \approx 2^{160}$ (ou $q \approx 2^{200}$, ou $q \approx 2^{256}$).
- $\#E(\mathbb{F}_q)$ presque premier.

Après les courses

On déduit des protocoles pour :

- l'échange de clés ;
- le chiffrement ;
- la signature.

(ici, on est dans le monde de la clé publique – crypto asymétrique).

Échange de clés

C’est le protocole de Diffie-Hellman classique.

Soit P un point sur la courbe E sur $\mathbb{F}_q$. P et E sont publics.

Alice	Bob
k_A au hasard	k_B au hasard

Échange de clés

C’est le protocole de Diffie-Hellman classique.

Soit P un point sur la courbe E sur $\mathbb{F}_q$. P et E sont publics.

Alice	Bob
k_A au hasard	k_B au hasard
$Q_A = k_A P$	$Q_B = k_B P$

Échange de clés

C’est le protocole de Diffie-Hellman classique.

Soit P un point sur la courbe E sur $\mathbb{F}_q$. P et E sont publics.

Alice		Bob
k_A au hasard		k_B au hasard
$Q_A = k_A P$	$\xrightarrow{Q_A}$	$Q_B = k_B P$
	$\xleftarrow{Q_B}$	

Échange de clés

C'est le protocole de Diffie-Hellman classique.

Soit P un point sur la courbe E sur $\mathbb{F}_q$. P et E sont publics.

Alice		Bob
k_A au hasard		k_B au hasard
$Q_A = k_A P$	$\xrightarrow{Q_A}$	$Q_B = k_B P$
secret $= k_A Q_B$	$\xleftarrow{Q_B}$	secret $= k_B Q_A$

$k_A k_B P$ est le secret commun

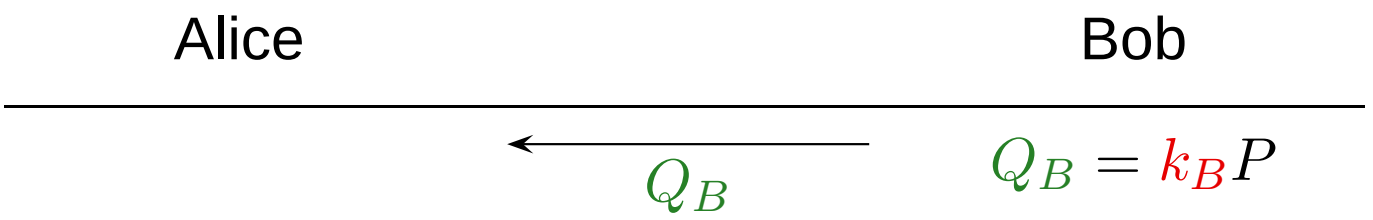
Un espion potentiel, connaissant Q_A et Q_B, ne peut déduire $k_A k_B P$.

$\Rightarrow$ Avec $k_A k_B P$, Alice et Bob établissent une communication sécurisée.

Chiffrement

Le chiffrement se fait par la méthode d'El Gamal (en gros).

- Pour tous : Une courbe E sur $\mathbb{F}_q$, un générateur P.
- Alice : clé secrète k_A, clé publique $Q_A = k_A P$.
- Bob veut chiffrer un message m pour Alice.



Chiffrement

Le chiffrement se fait par la méthode d'El Gamal (en gros).

- Pour tous : Une courbe E sur $\mathbb{F}_q$, un générateur P.
- Alice : clé secrète k_A, clé publique $Q_A = k_A P$.
- Bob veut chiffrer un message m pour Alice.

Alice		Bob
		$Q_B = k_B P$
	$\xleftarrow{Q_B}$	
		$C = \mathsf{E}_{k_B Q_A}(m)$
	$\xleftarrow{C}$	

$m = \mathsf{D}_{k_A Q_B}(C)$

Chiffrement

Le chiffrement se fait par la méthode d'El Gamal (en gros).

- Pour tous : Une courbe E sur $\mathbb{F}_q$, un générateur P.
- Alice : clé secrète k_A, clé publique $Q_A = k_A P$.
- Bob veut chiffrer un message m pour Alice.

Alice		Bob
		$Q_B = k_B P$
	$\xleftarrow{Q_B, C}$	$C = \mathsf{E}_{k_B Q_A}(m)$
$m = \mathsf{D}_{k_A Q_B}(C)$		

Chiffrement (suite)

À noter :

- (Q_B, C) est plus long que le message m.
- Le chiffrement requiert deux exponentiations.

  À titre de comparaison, RSA : $m^e \bmod N$, avec e petit.

Signature : (EC)DSA

Pour la signature, on adapte l'algorithme DSA, qui nécessite :

- Un groupe $\mathsf{G} = \langle P \rangle$, de cardinal q.
- Une fonction arbitraire $\phi : \mathsf{G} \to \mathbb{Z}/q\mathbb{Z}$ (pas trop moche).
- Une fonction de hachage H.
- Clé publique d'Alice : $Q_A = k_A P$.

Signature de m = couple (r, s) tel que :

- $T = \lambda P$, $r = \phi(T)$,
- $s = \lambda^{-1}(H(m) + rk_A)$.

Vérification de (m, r, s) :

$$\phi\left(s^{-1}(H(m)P + rQ_A)\right) \stackrel{?}{=} r.$$

car $\phi\left(s^{-1}(H(m)P + rk_A P)\right) = \phi\left(s^{-1}(H(m) + rk_A)P\right) = \phi\left(\lambda P\right).$

Signature : (EC)DSA (suite)

On veut atteindre un « niveau de sécurité » 2^η.

(EC)DSA est sûr si :
- le problème LD est difficile dans G,
- $\sqrt{q} > 2^\eta$.

Courbes elliptiques : à niveau de sécurité égal, groupe plus petit.

η	c.ell.	RSA/corps finis
80	160	1024
112	224	2048
128	256	3072

Comparaison en vitesse

L'avantage des CE grandit avec le paramètre η.

Ordre de grandeur du débit en logiciel ($\gg$ = plus rapide).

- $\eta = 80$: encrypt/verify$_{RSA}$ $\gg$ encrypt/verify$_{ECC}$ $>$ encrypt/verify$_{\mathbb{F}_q}$.
  decrypt/sign$_{ECC}$ $\gg$ decrypt/sign$_{RSA}$ $\gg$ decrypt/sign$_{\mathbb{F}_q}$.
- $\eta = 128$: encrypt/verify$_{RSA}$ $>$ encrypt/verify$_{ECC}$.
  decrypt/sign$_{ECC}$ $\ggg$ decrypt/sign$_{RSA}$.

1. Factorisation par la méthode des courbes elliptiques
2. Applications immédiates des courbes en cryptologie
3. Couplages
   - Définition, calcul
   - Applications des couplages
   - Sécurité des protocoles utilisant des couplages

Couplages

Les courbes permettent des opérations originales.

Couplage :
$$\begin{array}{ccc} \mathbb{G}_1 \times \mathbb{G}_2 & \longrightarrow & \mathbb{G}_3, \\ (P, Q) & \longmapsto & e(P, Q). \end{array}$$

Propriétés :
- linéaire en chaque variable : $e(P + P', Q) = e(P, Q)e(P', Q)$.
- non dégénéré.

Notre contexte :
- $(\mathbb{G}_1, +), (\mathbb{G}_2, +), (\mathbb{G}_3, \times)$,
- $\mathbb{G}_i$ cycliques, ordre ℓ premier.

Couplages sur les courbes elliptiques

Le couplage de Tate sur une courbe est lié à la ℓ-torsion.

Soit E définie sur $\mathbb{F}_q$, et ℓ premier $\neq \mathrm{char}(\mathbb{F}_q)$. On suppose :

- $\ell \,||\, \#E(\mathbb{F}_q)$: $E(\mathbb{F}_q)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$.
- $k > 1$ est l'ordre de q modulo ℓ. ($\ell \mid q^k - 1$).

Alors :

$$E(\mathbb{F}_{q^k})[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2.$$

Le couplage de Tate :

$$E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell.$$

- $\mathbb{G}_1 = E(\mathbb{F}_{q^k})[\ell]$: les points de ℓ-torsion. On peut se limiter à $E(\mathbb{F}_q)[\ell]$.
- $\mathbb{G}_2 = E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$. Pour fixer les idées, $= \mathbb{G}_1$ (pas toujours vrai).

pt de ℓ-torsion $\times$ pt de ℓ-torsion $\longrightarrow$ élément de $\mathbb{F}_{q^k}^*$.

Couplages sur les courbes elliptiques

Le couplage de Tate sur une courbe est lié à la ℓ-torsion.

Soit E définie sur $\mathbb{F}_q$, et ℓ premier $\neq \mathrm{char}(\mathbb{F}_q)$. On suppose :

- $\ell \,||\, \#E(\mathbb{F}_q)$: $E(\mathbb{F}_q)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$.
- $k > 1$ est l'ordre de q modulo ℓ. ($\ell \mid q^k - 1$).

Alors :

$$E(\mathbb{F}_{q^k})[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2.$$

Le couplage de Tate :

$$E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell.$$

- $\mathbb{G}_1 = E(\mathbb{F}_{q^k})[\ell]$: les points de ℓ-torsion. On peut se limiter à $E(\mathbb{F}_q)[\ell]$.
- $\mathbb{G}_2 = E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$. Pour fixer les idées, $= \mathbb{G}_1$ (pas toujours vrai).

pt de ℓ-torsion sur $\mathbb{F}_q$ $\times$ pt de ℓ-torsion sur $\mathbb{F}_{q^k}$ $\longrightarrow$ élément de $\mathbb{F}_{q^k}^*$.

Calcul du couplage de Tate

$$\underset{\text{sur } \mathbb{F}_q}{\text{pt de } \ell\text{-torsion}} \times \underset{\text{sur } \mathbb{F}_{q^k}}{\text{pt de } \ell\text{-torsion}} \longrightarrow \text{élément de } \mathbb{F}_{q^k}^*,$$

$$(P, Q) \longmapsto e(P, Q) \stackrel{\text{def}}{=\!=} f_{\ell,P}(Q).$$

Pour définir ce qu'est $f_{\ell,P}(Q)$, on doit parler de fonctions et de diviseurs.

Interlude – fonctions et diviseurs

- Une courbe $E : y^2 = x^3 + ax + b$ sur $\mathbb{F}_q$.
- Diviseurs : Sommes formelles de points sur E. $(P) + 42(Q) - 23(\infty)$
- Degré d'un diviseur : somme des multiplicités. 20
- Fonction sur la courbe : fraction rationnelle modulo E.
- Diviseur d'une fonction : $\sum$ zéros $-\sum$ pôles. $\Rightarrow$ diviseurs principaux.

On a :

- $\deg \operatorname{div}(f) = 0$.
- $\mathrm{Div}_0(E)$ est un groupe. $\mathrm{Princ}(E)$ sous-groupe.
- $\mathrm{Pic}_0(E) = \mathrm{Div}_0(E)/\mathrm{Princ}(E)$ est le groupe des points de E.

$$\text{« } P + Q = R \text{ »}$$

$$\Updownarrow$$

$$\exists f,\ \operatorname{div}(f) = [(P) - (\infty)] + [(Q) - (\infty)] - [(R) - (\infty)]$$

Calcul du couplage de Tate

$$\underset{\text{sur } \mathbb{F}_q}{\text{pt de } \ell\text{-torsion}} \times \underset{\text{sur } \mathbb{F}_{q^k}}{\text{pt de } \ell\text{-torsion}} \longrightarrow \text{élément de } \mathbb{F}_{q^k}^*,$$

$$(P, Q) \longmapsto e(P, Q) \overset{\text{def}}{=\!=} f_{\ell,P}(Q).$$

$f_{\ell,P}$ définie par :

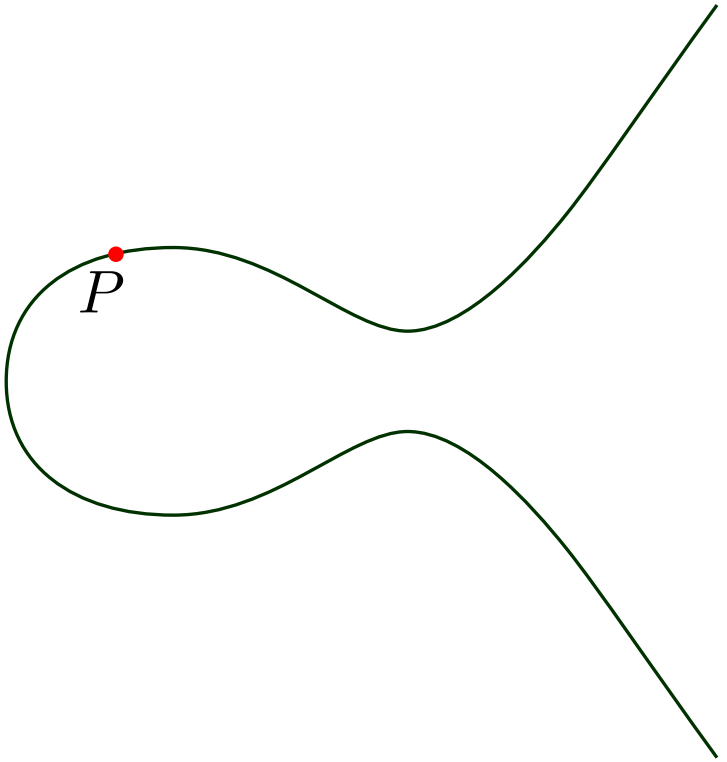
$$\operatorname{div} f_{\ell,P} = \ell\,[(P) - (\infty)] - [(\ell P) - (\infty)]\,.$$

$f_{\ell,P}$ est une fonction sur la courbe, on peut l'évaluer en Q.

Combien ça coûte ?

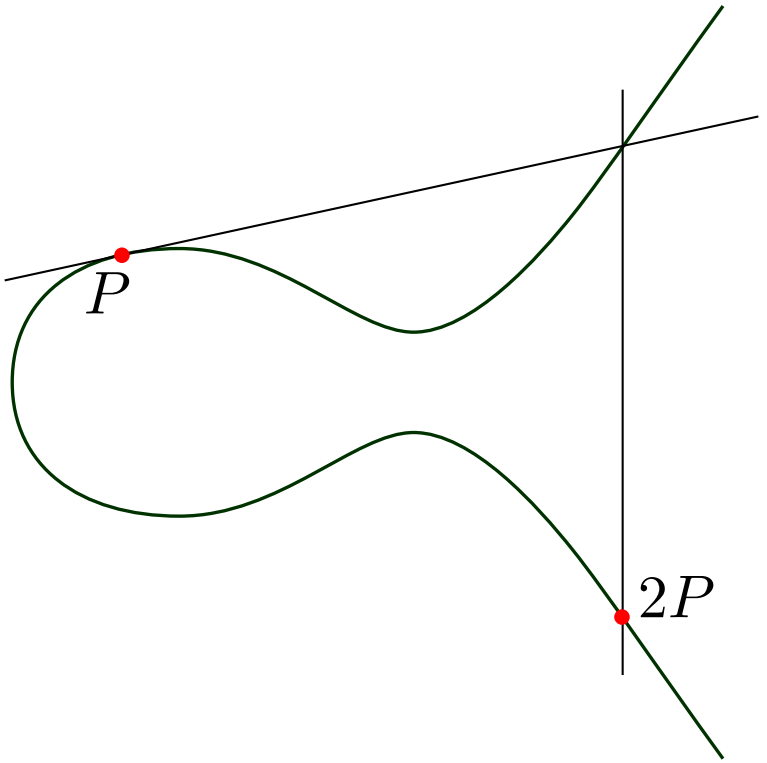
On recherche $f_{\ell,P} = \ell(P) - (\ell P) + \cdots$

Exemple : suivons le calcul de $13P$.



On recherche $f_{\ell,P} = \ell(P) - (\ell P) + \cdots$

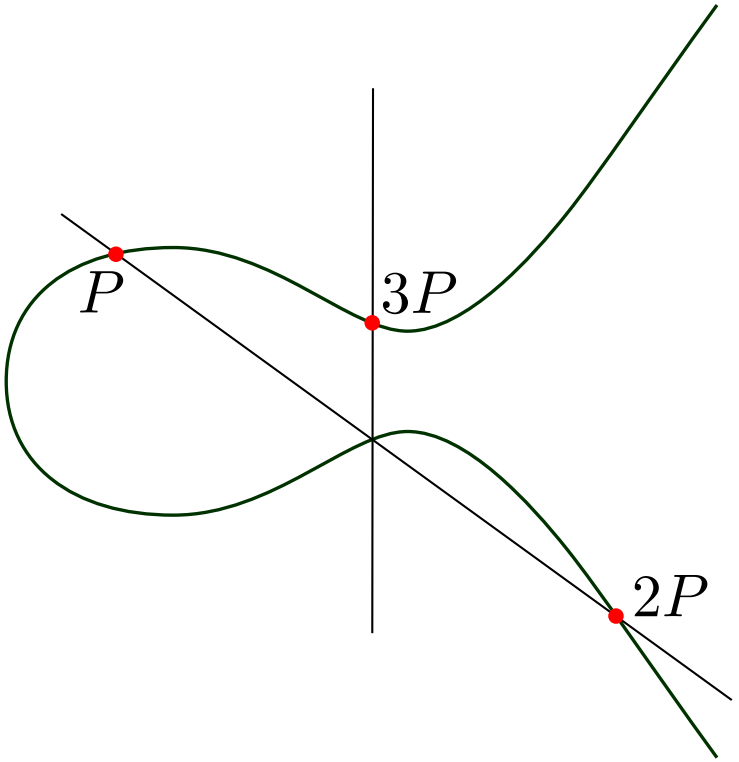
Exemple : suivons le calcul de $13P$.



$$\begin{aligned}
\operatorname{div} \lambda_2 &= 2(P) + (*) + \cdots, \\
\operatorname{div} v_2 &= (2P) + (*) + \cdots, \\
\operatorname{div} \frac{\lambda_2}{v_2} &= 2(P) - (2P) + \cdots, \\
\Rightarrow f_2 &= \frac{\lambda_2}{v_2}.
\end{aligned}$$

On recherche $f_{\ell,P} = \ell(P) - (\ell P) + \cdots$

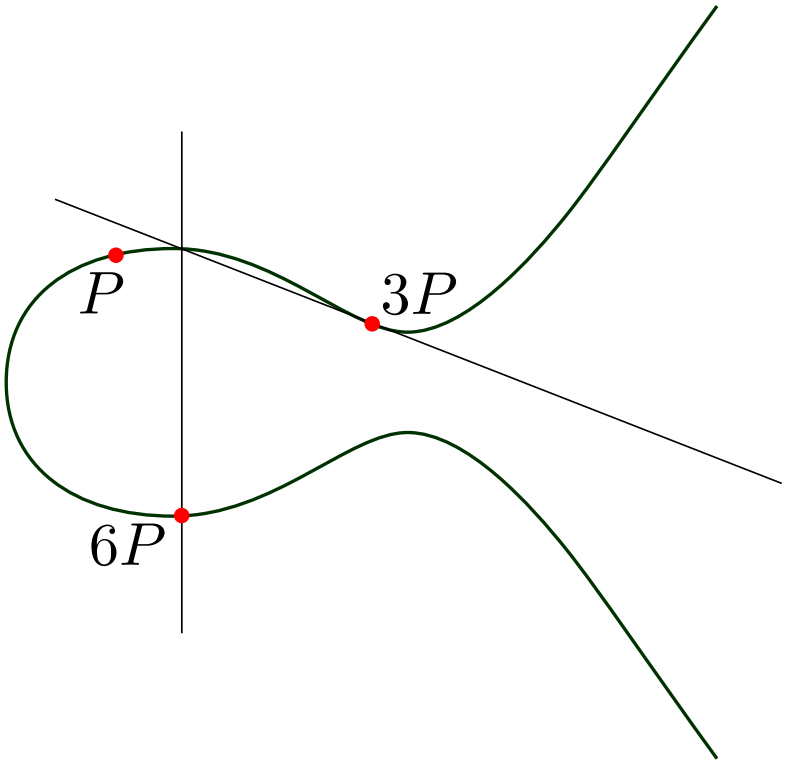
Exemple : suivons le calcul de $13P$.



$$\begin{aligned}
\operatorname{div} \lambda_3 &= (P) + (2P) + (*) + \cdots, \\
\operatorname{div} v_3 &= (3P) + (*) + \cdots, \\
\operatorname{div} \frac{\lambda_3}{v_3} &= (P) + (2P) - (3P) + \cdots, \\
\operatorname{div} f_2 \frac{\lambda_3}{v_3} &= 3(P) - (3P) + \cdots, \\
\Rightarrow f_3 &= f_2 \frac{\lambda_3}{v_3}.
\end{aligned}$$

On recherche $f_{\ell,P} = \ell(P) - (\ell P) + \cdots$

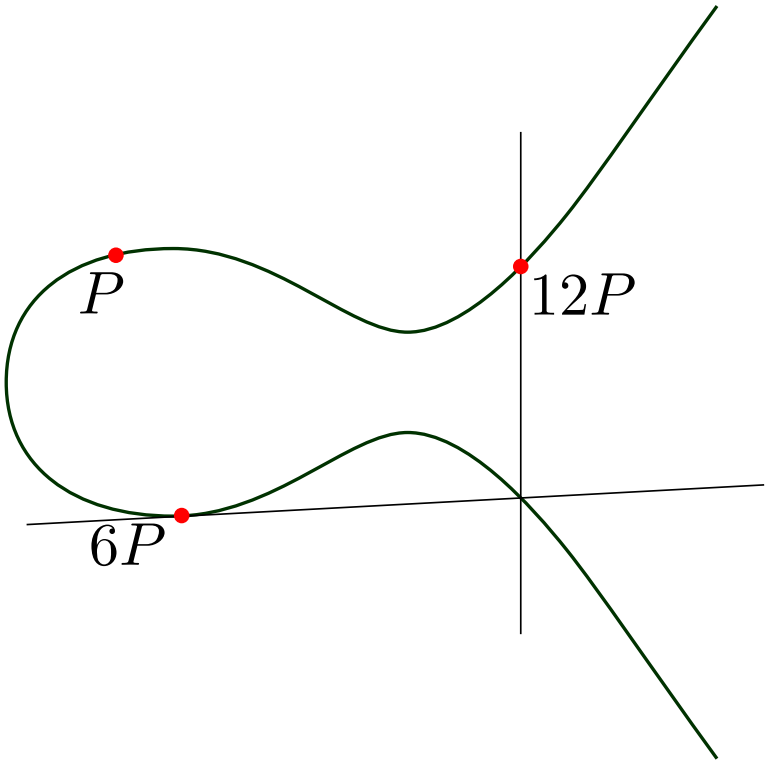
Exemple : suivons le calcul de $13P$.



$$\begin{aligned}
\operatorname{div} \lambda_6 &= 2(3P) + (*) + \cdots, \\
\operatorname{div} v_6 &= (6P) + (*) + \cdots, \\
\operatorname{div} \frac{\lambda_6}{v_6} &= 2(3P) - (6P) + \cdots, \\
\operatorname{div} f_3^2 \frac{\lambda_6}{v_6} &= 6(P) - (6P) + \cdots, \\
\Rightarrow f_6 &= f_3^2 \frac{\lambda_6}{v_6}.
\end{aligned}$$

On recherche $f_{\ell,P} = \ell(P) - (\ell P) + \cdots$

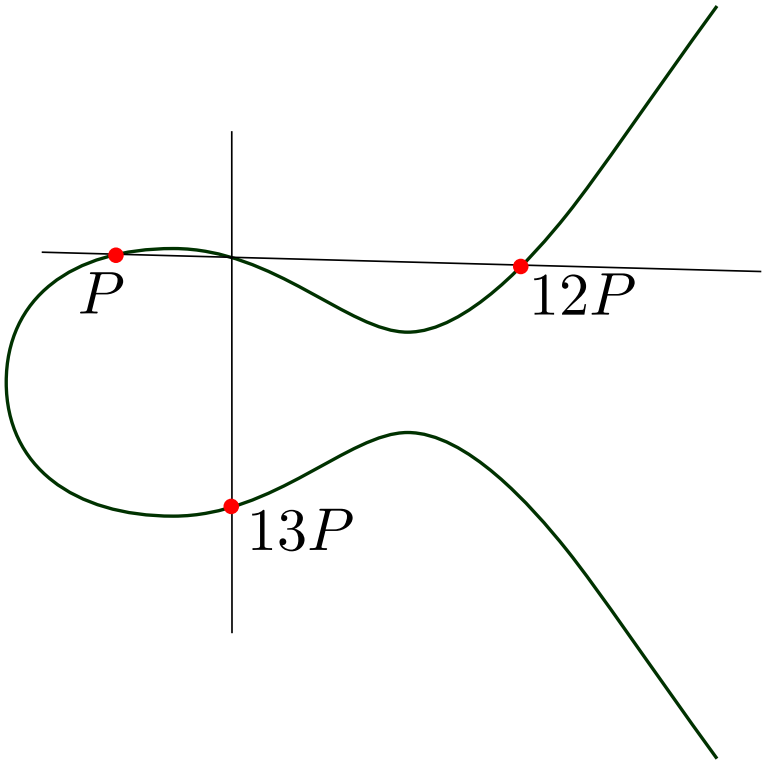
Exemple : suivons le calcul de $13P$.



$$\begin{aligned}
\operatorname{div} \lambda_{12} &= 2(6P) + (*) + \cdots, \\
\operatorname{div} v_{12} &= (12P) + (*) + \cdots, \\
\operatorname{div} \frac{\lambda_{12}}{v_{12}} &= 2(6P) - (12P) + \cdots, \\
\operatorname{div} f_6^2 \frac{\lambda_{12}}{v_{12}} &= 12(P) - (12P) + \cdots, \\
\Rightarrow f_{12} &= f_6^2 \frac{\lambda_{12}}{v_{12}}.
\end{aligned}$$

On recherche $f_{\ell,P} = \ell(P) - (\ell P) + \cdots$

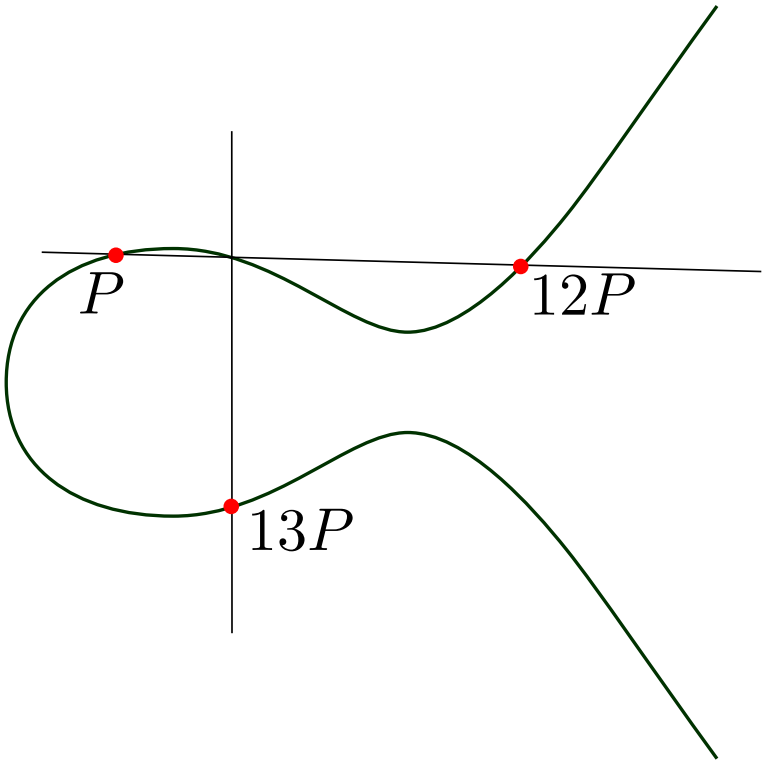
Exemple : suivons le calcul de $13P$.



$$\begin{aligned}
\operatorname{div} \lambda_{13} &= (P) + (12P) + (*) + \cdots, \\
\operatorname{div} v_{13} &= (13P) + (*) + \cdots, \\
\operatorname{div} \frac{\lambda_{13}}{v_{13}} &= (P) + (12P) - (13P) + \cdots, \\
\operatorname{div} f_{12}\frac{\lambda_{13}}{v_{13}} &= 13(P) - (13P) + \cdots, \\
\Rightarrow f_{13} &= f_{12}\frac{\lambda_{13}}{v_{13}}, \\
&= \left(\left(\frac{\lambda_2}{v_2}\frac{\lambda_3}{v_3}\right)^2 \frac{\lambda_6}{v_6}\right)^2 \frac{\lambda_{12}}{v_{12}}\frac{\lambda_{13}}{v_{13}}.
\end{aligned}$$

On recherche $f_{\ell,P} = \ell(P) - (\ell P) + \cdots$

Exemple : suivons le calcul de $13P$.



$$\begin{aligned}
\operatorname{div} \lambda_{13} &= (P) + (12P) + (*) + \cdots, \\
\operatorname{div} v_{13} &= (13P) + (*) + \cdots, \\
\operatorname{div} \frac{\lambda_{13}}{v_{13}} &= (P) + (12P) - (13P) + \cdots, \\
\operatorname{div} f_{12}\frac{\lambda_{13}}{v_{13}} &= 13(P) - (13P) + \cdots, \\
\Rightarrow f_{13} &= f_{12}\frac{\lambda_{13}}{v_{13}}, \\
&= \left(\left(\frac{\lambda_2}{v_2}\frac{\lambda_3}{v_3}\right)^2 \frac{\lambda_6}{v_6}\right)^2 \frac{\lambda_{12}}{v_{12}}\frac{\lambda_{13}}{v_{13}}.
\end{aligned}$$

$\Rightarrow$ Calculer $f_{\ell,P}$ est similaire au calcul de ℓP.

$\Rightarrow$ Pour $f_{\ell,P}(Q)$, on évalue à chaque étape.

Moralité sur le calcul du couplage

- $f_{\ell,P}(Q)$ se calcule bien.
- On calcule en fait $(f_{\ell,P}(Q))^{(q^k-1)/\ell}$ pour atteindre une racine de l'unité.
- $Q \in E(\mathbb{F}_{q^k})$.
- Mille et mille variantes et améliorations.

Moralité : quand un couplage existe, il se calcule.

Casser LD

On a dit que LD est difficile sur E.

Si on a un couplage $E[\ell] \to \mathbb{F}_{q^k}$:

$$e(\ell P, Q) = e(P, Q)^{\ell}.$$

Si on sait résoudre LD dans $\mathbb{F}_{q^k}^*$, on sait résoudre LD dans E.

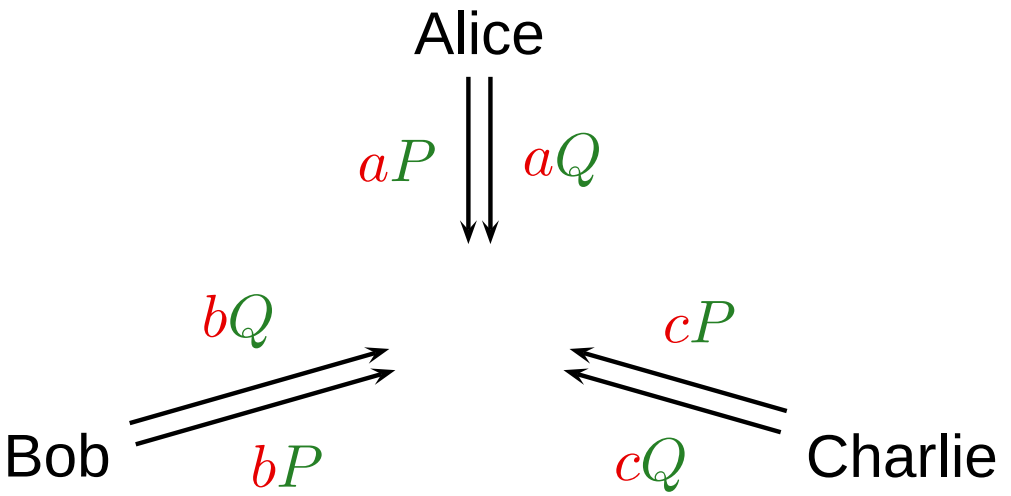
Pour k petit, peut permettre de calculer LD dans E plus vite.

Diffie-Hellman à trois

Diffie-Hellman : échange de clés à deux.

Avec les couplages, on peut faire à trois.

Contexte : une courbe E, un couplage, et P, Q tels que $e(P,Q) \neq 1$.

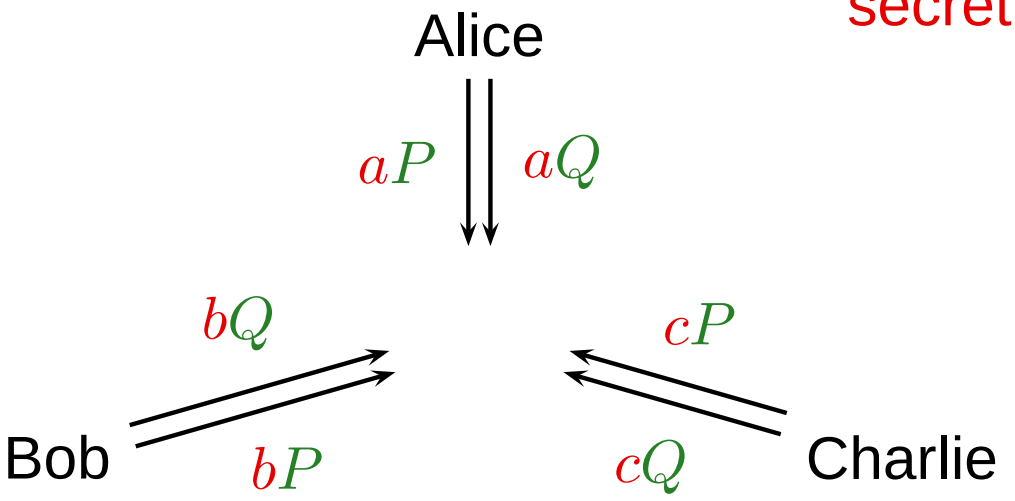


Diffie-Hellman à trois

Diffie-Hellman : échange de clés à deux.

Avec les couplages, on peut faire à trois.

Contexte : une courbe E, un couplage, et P, Q tels que $e(P,Q) \neq 1$.



secret $= e(bP, cQ)^a$
$= e(P,Q)^{abc}$

secret $= e(aP, cQ)^b$

secret $= e(aP, bQ)^c$

« Identity-based encryption » (IBE)

Pour chiffrer, on a besoin de connaître la clé publique.

Alice		Bob
		$Q_B = k_B P$
$m = \mathsf{D}_{k_A Q_B}(C)$	$\xleftarrow{Q_B, C}$	$C = \mathsf{E}_{k_B Q_A}(m)$

Objectif IBE : utiliser seulement l'identité : `alice@fai.com`

Outils :
- Une courbe, un couplage, un point $P \in E(\mathbb{F}_q)$.
- Une fonction H : *chaîne de bits* $\to E(\mathbb{F}_{q^k})$.
- On ne veut pas de gag avec $e(P, H(\mathsf{id}))$.

Protocole de Boneh-Franklin

Une autorité
- détient un secret maître $s \in \mathbb{Z}/\ell\mathbb{Z}$.
- publie $P, Q \in E(\mathbb{F}_q)$, avec $Q = sP$.
- vend sa clé secrète à Alice : $S_A = sH(\mathsf{id}_{\mathsf{Alice}})$.

Alice		Bob
		$y = e(H(\mathsf{id}_{\mathsf{Alice}}), Q)$
		$T = rP$
$m = \mathsf{D}_{e(S_A,T)}(C)$	$\xleftarrow{T, C}$	$C = \mathsf{E}_{y^r}(m)$

$$e(S_A, T) = e(sH(\mathsf{id}_{\mathsf{Alice}}), rP) = e(H(\mathsf{id}_{\mathsf{Alice}}), sP)^r = y^r.$$

Hypothèses de sécurité

Les protocoles supposent que :

- LD est difficile dans E : $(Q = sP, P) \longrightarrow\!\!\!\!\!\!\times\ s$.
  - Attaques exponentielles.
  - $\#E(\mathbb{F}_q) \approx 2^{160}$ mini.
- LD est difficile dans $\mathbb{F}_{q^k}^*$: $(e(rP, R) = e(P, R)^r, e(P, R)) \longrightarrow\!\!\!\!\!\!\times\ r$.
  - Attaques sous-exponentielles.
  - $q^k \approx 2^{1024}$ mini.

Pour des raisons d'efficacité, on aime tomber juste.

- Aujourd'hui (hier), $k = 6$ bien.
- Aujourd'hui (demain), k un peu plus grand (8, 10).
- On aime pouvoir construire des courbes avec k contraint.

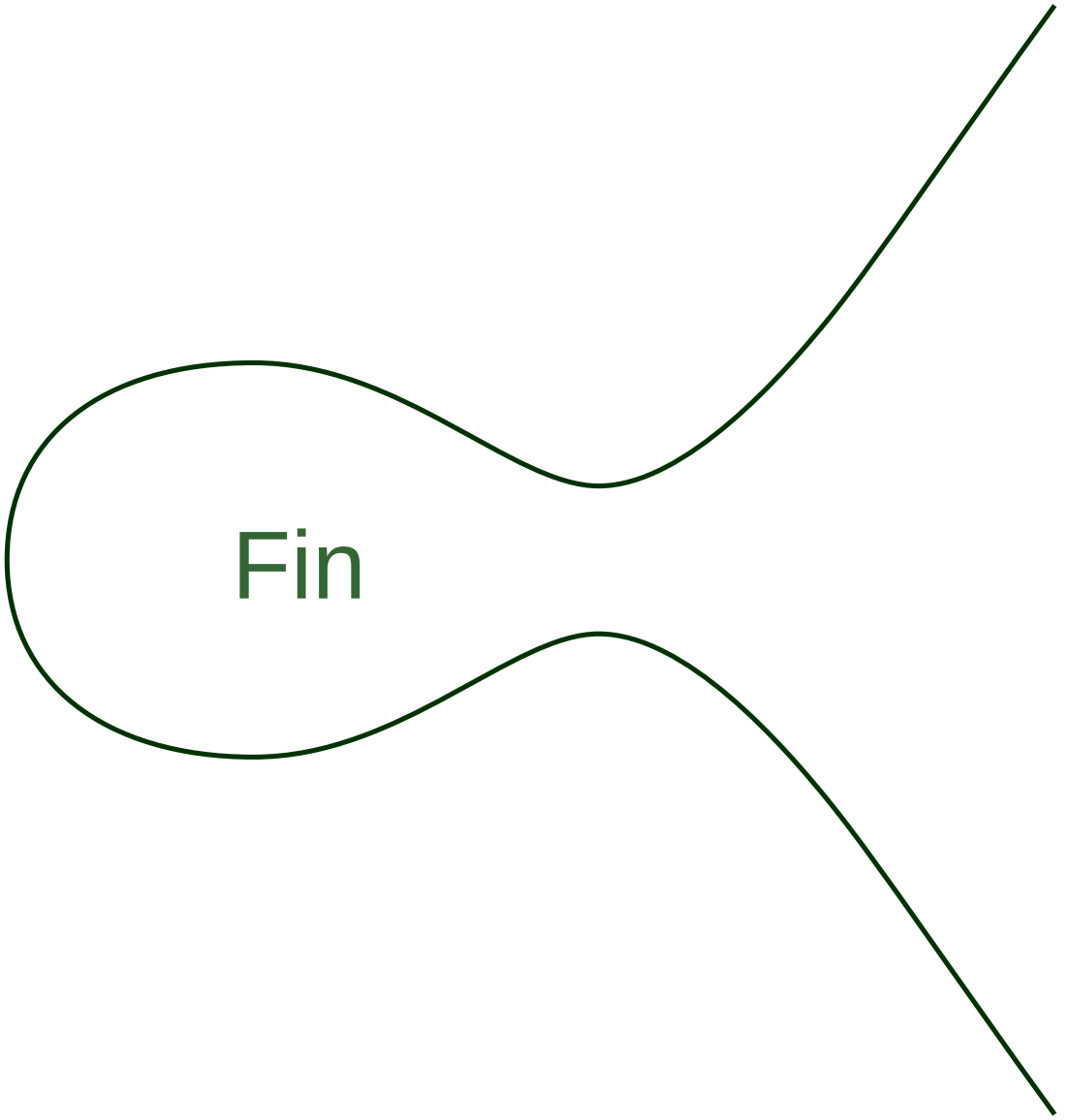
Conclusion

Les courbes elliptiques ont plein d'applications.

- La structure est riche, les opérations sont riches.
- Applications notamment en crypto.

Au-delà : courbes de genre supérieur.

- On n'opère plus sur des points, mais sur des diviseurs.
- Beaucoup de choses se généralisent, pas tout.


Fin